Internet Acceptable Use Policies:

Navigating the Management, Legal and Technical Issues

By
Farley Stewart, VP of Internet Appliance Products
St. Bernard Software, Inc.

Table of Contents

Internet Acceptable Use Policy

Over the past few years, providing employees with access to the Internet has become a critical factor in the success of most corporations and other large organizations in the United States and around the globe. Many companies have openly embraced the widespread use of the World Wide Web, Internet e-mail, and file transfer mechanisms as highly efficient communications and research tools to boost employee productivity. In addition, a rapidly growing number of organizations are also instituting private intranets and extranets to enhance their employees' internal communications and to streamline interaction with external customers and partners. Each day more employers are granting their employees' access to the Internet in order to take advantage of the wide range of readily available information and to improve the overall efficiency of their internal and external operations.

However, too many organizations have also discovered the hard way that unrestricted and unmanaged Internet access by employees can lead to dire consequences in the form of wasted time, lost productivity, misappropriation of resources, reduced morale, and the risk of diminished corporate reputation. Perhaps more importantly, an organization's failure to take adequate steps to define, manage and control employees' Internet usage can also lead to severe risks in the form of potential legal and financial liabilities.

The need to protect against these risks has given rise to a whole new wave of significant management efforts involving corporate executives, IT managers, human resource staff and the legal community. Although the need for comprehensive and enforceable Internet Acceptable Use Policies (IAUP) has now become a critical issue cutting across organizations in virtually all industry segments, all too often the IAUP policy efforts or technological implementation for policy enforcement fall short of the mark.

In some cases, the shortcoming is because company management fails to understand the full extent of the risk, while in other instances there is reluctance to come across like "big-brother" for fear of harming the company culture. Sometimes IAUP efforts fail to adequately address the legal issues involved and other times the policies are simply ignored because they are too full of "legalese" to be understood by rank-and-file managers and employees. Or, even with extremely well intentioned and well-crafted IAUPs, the failure to deploy appropriate technologies for comprehensive monitoring and management can dilute the policy's enforceability or, on the other end of the scale, can severely restrict Internet usability to the point of compromising its overall benefits.

The bottom line is that an effective IAUP must take into account the whole spectrum of these policy and technology issues, within the framework of the specific organization's unique set of goals and culture. During the balance of this article, we will take a closer look at the benefits and risks of employee Internet usage and then will explore the specific issues involved in the development and deployment of effective IAUPs and how to enforce them.

When it comes to potential employee abuse of their Internet access, the most prominent concerns are loss of productivity, degradation of available computing resources and the high risks of legal liabilities — for example, those associated with sexual or other types of harassment based upon access and display of inappropriate web content.

Loss of Productivity

The potential negative impacts from lost productivity alone represent a multi-billion dollar issue for today's companies. According to estimates by research firm Computer Economics, companies lost $5.3 billion to recreational Internet surfing in 1999. As Michael Erbschloe, Computer Economics vice president of research, describes it, "Online shopping, stock trading, car buying, looking for a new house, and even visiting porn sites have become daily practices for about 25 percent of the workers in U.S. companies that have access to the Internet in their offices. The illegitimate and personal use of the Web by employees has become commonplace. And when the boss is not around, improper use of the Web is normal. The inappropriate activities even include employees starting their own e-business operations and building and promoting their own Web sites while in the office of their full-time employer."

For the most part, organizations that provide their employees with Internet access expect that there will be some small amount of personal use. In concept, this is not much different than the traditional issue of allowing some "reasonable" amount of personal calls using company telephones. In practice, however, the Internet poses a much more sweeping opportunity for abuse. For example, an employee's Web browsing for a quick ad hoc check of the stock market might seem innocuous enough on the surface, but what about when the lure of the Web draws that same employee to expand their activities to continual tracking of quotes, in-depth research and online day trading?

As most of us have discovered from time to time in our home-based Web browsing, it's very easy to start off with a single objective and then, through the magic mix of hyperlinks and human curiosity, we find ourselves exploring interesting new areas that we had never previously considered. To a significant extent, it is exactly that "unlimited diversity at your fingertips" phenomena that makes the Web so compelling for millions of users. Unfortunately, as a growing body of research is showing, the availability of compelling content can turn into compulsive behavior for a significant percentage of Web users. While it is easy to understand how an otherwise valued employee might inadvertently slip into a pattern of misuse, in the long run it is incumbent upon the employer to anticipate such risks and to establish well-communicated policies and management mechanisms to help employees live up to required expectations.

If left unchecked, even a small amount of Internet abuse by only a few employees can easily turn into a widespread pattern of abuse, making it the norm. In certain situations, the misuse of web browsing privileges can actually become a self-reinforcing social phenomena in which even those employees who would not typically flaunt the rules eventually also succumb to the "everybody's doing it" attitude. For example, after the peak of the Clinton-Lewinsky scandals, ZDNet reported that industry experts estimated "American companies lost $470 million in productivity to employees reading the salacious document online."

Drain on Computing Resources and Bandwidth

Besides the loss of productivity for the employees that are directly abusing their Internet access privileges, another major concern involves the ripple effects of clogged bandwidth, degraded system performance and over-consumption of finite computing resources that can indirectly reduce the productivity of other non-abusing employees. In some cases, the ripple effects can be catastrophic. Consider the PointCast stir a few years back. Businesses were stunned to find that almost overnight significant percentages of their employees with access to the Internet were getting large quantities of real time data — news stories, stock ticker data — being 'pushed' to their desktops. They were experiencing double-digit percentage loss of bandwidth without even seeing it coming. Today, the same risk exists and is being manifested in the streaming audio, "free music over the Internet" phenomenon. While the music may be free to those who listen to it, it's not free to the employer who pays for the Internet connectivity. However, most of the time the performance-degrading impacts of misuse are more insidious by slowly choking off the company's networked computing resources, while masquerading as legitimate work-related traffic.

For most organizations, the networked IT infrastructure has evolved into an indispensable part of their everyday operations, providing the underlying foundation for everything from new product development to manufacturing to finance and human resources. In addition, with the rise of e-commerce in both the business-to-consumer and business-to-business arenas, many companies now also depend vitally upon the performance of their network to support responsive communications and real-time transactions with their customer base. When network performance is degraded, companies are often forced to respond with major new investments in system improvements and expanded bandwidth, even though they may be unaware that a significant part of the demand is coming from inappropriate Internet usage by employees.

The inappropriate consumption of bandwidth can greatly escalate with the ability of Internet users to set up "push" applications, in which the remote web sites automatically provide updates, such as stock quotes, news or auction bids, on a continuous basis. In a similar vein, workers may listen to streaming music or radio stations that broadcast over the Internet. In these instances, the employee may not realize the extent to which they have impacted the company's resources because they go on with their other activities, while no one on the IT staff is even aware that the push or streaming application is siphoning off scarce and costly network bandwidth.

Legal Liability Risks

Going beyond the concerns of loss of productivity and degradation of available network resources, many companies are just now coming to realize that the latent legal risks from employees' Internet abuse can potentially be astronomical. The major concern is the employer's obligation to take prudent steps to protect all employees from "hostile work environments" such as exposure to sexually oriented or hate-related information in the workplace.

As described by Frank C. Morris, Jr, director of the Employment Law Department at Epstein, Becker & Green in Washington D.C., "since the number of discrimination lawsuits have been on the rise, the workplace has become more politically correct. Rarely will employees engage in the same offensive conduct that was commonplace just a few years ago. As a result, potential plaintiffs have had to look elsewhere for 'smoking guns' to prove their cases, and many are now finding them with the increased presence of the Internet in the workplace."

Morris further explains, “Few employees would believe that their seemingly innocent Web-surfing could expose their employers to insurmountable liability. But it is this improper use of the Internet that is now the smoking “e-gun” of current plaintiffs. For a plaintiff, there is nothing better than walking into court with a piece of paper illustrating a discriminatory statement, joke or picture downloaded off the Internet and sent through e-mail.”

Even though enlightened management practices have virtually eliminated yesterday’s common practice of posting sexually oriented pictures on the walls of businesses, too many employees tend to think that the fleeting exposure of a similarly offensive picture on a computer screen is somehow not a problem. However, the courts have consistently held that the presence of Internet-related sexual content in the workplace does meet the definition of harassment and that the employer’s failure to take appropriate preventative measures does constitute a violation of an employees’ rights.

Besides hostile workplace concerns, a variety of other legal exposures can also accrue to employers through their employees’ misuse of the Internet. For instance, employers can also potentially be held liable for employees who use company Internet connections to violate copyright laws or to post false information that libels other companies or individuals. While the case law continues to evolve in this area, there is also some potential that a company could even be deemed responsible for illegal activities, such as fraudulent Internet scams, conducted by its employees if company equipment and Internet access were involved.

Beyond the strict legal liabilities, a company can also sustain significant damage to its reputation and goodwill as a result of the negative publicity that can ensue from employee misuse of the Internet. At best, the company can simply appear to be badly managed for allowing such practices or, worse yet, it can actually lose business from customers that are worried about lack of adequate controls and security.

Crafting an Organization-Specific Internet Acceptable Usage Policy

The creation of an effective Internet Acceptable Use Policy requires a comprehensive understanding of the company’s business goals, Internet usage objectives, specific risk profiles, and organizational culture. In most mid- to large-size organizations, the IAUP development effort must involve a high degree of cross-departmental inputs from the executive staff, human resources, IT management, and functional departmental managers.

According to Ira G. Rosenstein, a New York-based partner in the Employment Department of Orrick, Herrington & Sutcliffe, “the Internet is a valuable tool and therefore it is very important to craft the usage policy in such a way that it reinforces productivity and employee morale, without becoming unmanageable. For example, if a policy inflexibly mandates very draconian measures for the slightest infraction, it greatly reduces management’s ability to apply a measured or proportionate response to different types or levels of Internet abuses. With any policy covering areas that could be deemed the ‘personal’ activities of employees, it makes sense to build in some degree of discretion. However, in order to ensure that the policy is sufficiently enforceable, employers need to clearly define what does and does not constitute acceptable behaviors with regard to Internet usage.”

Rosenstein adds, “in some instances, a ‘zero-tolerance’ stance may be necessary, such as if an employee knowingly and repeatedly accesses pornographic or hate-inciting Web sites. Obviously, these offenses are very different than going to an e-commerce site and buying the latest *NY Times* best-selling novel, especially as it relates to the liability risks of litigation from other impacted employees. The ability to distinguish between ‘casual’ and ‘chronic’ behavior is also a useful concept to build into the policy. For instance, even relatively innocuous behavior can rise to the level of a serious offense if it becomes chronic, such as the difference between an employee quickly checking out an item on eBay or spending half a day bidding and tracking various auction items.”

As Frank Morris of Epstein, Becker & Green points out, “perhaps most importantly, it is critical to remember that an Internet usage policy cannot be treated as a ‘one size fits all’ proposition. In order to be truly effective, the policy has to fit within the corporate culture and goals while clearly conveying its underlying rationale in a manner that makes sense to the company’s employees. For example, while virtually no one would be likely to argue that any company’s employees need at-work access to porn sites, the range of Internet access needed in a web-centric e-commerce company is probably going to be wider than that required in the accounting department of a traditional manufacturing company.”

Notification, Education and Application

Of course, after the policy has been developed, it cannot actually become useful until it has been communicated to employees. In most companies, the initial notification takes the form of having each employee read the policy and sign an “acknowledgement of receipt” that then becomes a permanent part of their personnel file. In addition to the initial notification, it may also be prudent for the companies to include short educational sessions on Internet usage policies as a formal part of new-employee orientation and training curricula.

According to Ira Rosenstein, “essentially the company needs to inform every employee of the policy’s provisions as soon as they are given access to the Internet and then also to reinforce the employee’s obligations on a regular basis. For example, some companies set up a short summary of the policy as a ‘splash screen’ that appears for a brief period during boot-up and whenever an employee signs on to the Internet.”

Keeping in mind the overall corporate culture and ensuring that the Internet usage policy meshes smoothly within the existing management philosophies can also enhance overall understanding and compliance. The avoidance of overt legalese is important, as is the need to craft the notification methods to be consistent with other company policies. For example, while very firm and proscriptive language may be quite appropriate in some more traditional firms, it is less likely to be well received within the free-flowing environment of a web-centric technology company. Here again, it is important to keep in mind that the ultimate objective of the IAUP effort is not so much to catch people doing something wrong as it is to proactively prevent abuse through a well-crafted and well-communicated policy.

Technology Issues in Monitoring and Enforcement

Often the mere existence and promulgation of a clear policy is enough to stem most forms of Internet access abuse. At the very least, it provides a firm basis for communicating with employees whenever policy violations lead to the need for corrective action. However, like any rule that is not enforced, Internet access policies that are not backed up by proactive monitoring and access control measures will quickly become hollow pronouncements – losing both the ability to effectively guide users' behavior and to protect the organization from liability. Therefore, more organizations are turning to the dual strategy of publishing clear IAUPs combined with instituting comprehensive, precision Internet access control over user's Web related activities.

A May 1999 study conducted by Zona Research, showed that one-third of companies use some type of screening to block out employee access to sites that are not on an approved list. In its survey of more than 300 companies, Zona also found that 20 percent of the organizations use selective screening to filter sites based on the users' job categories while 13 percent selectively filtered based upon the time of day.

Over the past few years, the need to proactively control web access has driven the development of a variety of web-filtering methodologies, from plug-in software for the PC browser client to complex server software packages. However, the unrelenting growth of new Internet content combined with the need for transparent network installation and simple setup and administrative mechanisms to manage large numbers of users have often made these alternatives either too unwieldy and/or too ineffective for use by most businesses.

Early attempts at Internet access control focused primarily on filtering based upon keywords as the means to identify objectionable or inappropriate content. This method entailed scanning text on web pages received and matching them against lists of "bad" keywords. Given that many words can only be judged in context, these solutions had an impossible balancing act between filtering out too little or too much material. Besides the issue of inaccuracy, these keyword based solutions didn't protect companies or users from access to other forms of inappropriate Internet content, such as pornographic images or graphics.

A major improvement came with the introduction of solutions that monitor and/or block access based upon the Web site being requested. When human operators who work for the solution provider have a chance to make the call before placing a site in a blocked category list, most of the ambiguity and inaccuracy associated with the keyword approach is eliminated. With this approach, when a user clicks on a link or enters a Web site address, it is matched against a database of inappropriate sites. If the requested site is found on the list of blocked sites, the user is presented with a message stating that access to this site is contrary to company policy and who to contact if they think they have a legitimate reason for accessing that site.

Given the dynamic and explosive nature of the Internet, with thousands of new sites going online every day, this type of approach is only viable when coupled with a subscription service that continually provides updates for the database of inappropriate sites, preferably on a daily basis. And to ensure that the updates are applied as they are delivered, the filtering tool used should allow for automatic refresh of the database. Like a virus checker without the latest virus definitions applied, protection rapidly diminishes. Daily updates need to be delivered and applied over the Internet for the best protection and to save administrators a great deal of effort. Weekly or monthly CD update lists that sit on someone’s desk sap a company of the protection they have paid for.

When considering a database driven solution, there are two primary types. The first blocks based upon a requested Web site’s IP address (ex: http://199.42.53.141/). The second alternative blocks based upon the site’s URL address (ex: www.mycompany.com). The URL approach solves a unique problem associated with the IP address approach. When blocking by IP address, all web sites that share an IP address, as is the case with many hosted web sites, get blocked with the one offender. Using URLs, targeted hosted sites can not only be singled out, but specific sections of sites and even individual pages can be identified and blocked.

Regardless of the blocking approach, a filtering solution must be flexible. Not only does an IAUP need to adapt to a company’s culture and specific needs, but so does the tool to enforce that policy. IT administrators need the ability to custom tailor and control their filtering rules and databases. Local control of how site categories and specific sites are rated and handled is very important. The ability to tailor blocking on a group-by-group or individual user basis is needed. And being able to control access based upon time of day or day of week is becoming increasingly important.

Flexibility is also needed in the range of Internet services controlled. As the variety and type of Internet content have proliferated, the issue of access control has now expanded way beyond just HTML-based web pages. Unauthorized access to other Internet services, such as ICQ® and IRC chat, FTP downloads, RealAudio® broadcasts and MP3 music, can easily consume significant bandwidth and resources while degrading employee productivity, all without triggering any access control mechanisms in traditional web filtering products.

Finally, in order to be truly effective, Internet access management technology must not only be accurate, dynamic, automatic, tailorable and comprehensive, but affordable, transparent to the installed network hardware and software, easy to set up and maintain, non-performance degrading and scalable enough to grow with the corporate IT environment. In response to these needs, a new generation of turnkey solution is just now emerging— the Internet filtering server appliance. These are dedicated, low cost, solid state devices that can be dropped into virtually any network. By their nature, they can begin providing filtering protection straight from the box, yet allow for easy customization to meet just about any enterprise's needs. The best require no modification to existing desktop browsers or network servers.

By combining subscription-based filtering services with the easy installation and administration of “plug-and-protect” server appliances, these new alternatives provide highly customizable filtering mechanisms and user profiles, sophisticated monitoring and filtering of all Internet content types, plus a high degree of scalability and maintainability.

Bottom Line

Given the risk of legal liability, productivity loss and bandwidth drain, it is clear why an Internet Acceptable Use Policy is needed by companies today. It is also important that the IAUP be tailored to meet the needs of each organization – one size does not fit all. If the policies are too restrictive or too lax they run the risk of causing an employee backlash or providing inadequate corporate protection.

Once an IAUP is established, employee communication is critical. If the employees are not clearly notified and educated as to the policy requirements, they will lack the knowledge base needed to fully comply.

Tools are then needed to help ensure compliance by all employees. Without the tools or means to monitor and enforce the policy, an IAUP will become toothless and not provide the protection desired. Like the usage policies themselves, a company's monitoring and control mechanisms must also be tailorable to meet the specific requirements of the organization and include the capability for evolving and adapting with changing requirements.

Ultimately, the organization's Internet Acceptable Use Policies, management/supervision practices, employee training/education programs, and the Internet access management technologies all have to mesh together to form a unified and proactive system for effectively managing all employees' online behavior.

For more information please contact us at 1-800-782-3762 or 858-676-2277.

Biographical information:

Farley Stewart, VP of Internet Appliance Products at San Diego-based St. Bernard Software, Inc., is an Internet pioneer who, has lead the drive to simplify the difficult process of establishing and managing an organization’s Internet presence. St. Bernard Software manufactures a unique new server appliance called iPrism that monitors and filters employee Internet access (iPrism debuted October 25, 1999). Development of other server appliances is anticipated. Farley has some 16 years of business experience that includes software development, engineering, sales, marketing and executive management. Farley holds a Bachelor of Science degree in electrical engineering with emphasis on communication systems from the University of California, San Diego.

###